acopia NETWORKS

Adaptive infrastructure. On-demand.

GUI Quick Start: Network Setup

Part Number: 810-0042-00, Revision D

Acopia Networks®, Inc.
41 Wellman Street
Lowell, MA 01851
(978) 513-2900 tel
(978) 513-2990 fax

GUI Quick Start: Network Setup

Copyright© 2006-2007, Acopia Networks®, Inc. Third-party copyrights appear in *Copyrights*.

All Rights Reserved, Printed in U.S.A.

Revision History

June 2006 - Rev A
October 2006 - Rev B, change links to CLI User's guides
October 2006 - Rev C, Software Release 2.4.2
March 2007 - Rev D, Software Release 2.5.0
June 2007 - Rev E, Software Release 2.5.1; change title

The information in this document is proprietary to Acopia Networks®, Inc. Any unauthorized reproduction, distribution, or use of this material is strictly prohibited.

Acopia Networks®, Inc. assumes no responsibilities for any inaccuracies that may appear within this document. In no event will Acopia Networks be liable for direct, indirect, special, exemplary, incidental, or consequential damages resulting from any defect or omission within this document.

Acopia Networks®, Inc. reserves the right to alter the contents of this document at any time, and without any notice.

The terms and conditions for using the products are described in the license agreement that either shipped with the products, was contained in the acknowledgement to your purchase order, or was otherwise provided to you. If you have any questions about the license terms, please contact your Acopia Networks representative. By using the products you indicate that you understand and agree to be bound by the terms and conditions of the license agreement.

The ARX's Licensed Software includes object code versions of third party software packages. These software packages are subject to the terms and conditions of the license agreements found at http://www.apache.org/licenses/LICENSE-2.0; http://www.gnu.org/licenses/gpl.html; http://www.gnu.org/licenses/lgpl.html; ftp://ftp.isc.org/isc/inn/inn-2.4.1.tar.gz (the license file is inn-2.4.1/LICENSE).

FreedomFabric™ is a trademark and ARX® is a registered trademark of Acopia Networks, Inc. All other brands, products, or service names may be trademarks or service marks of the companies with which they are associated.

GUI Quick Start: Network

Use this document to connect to the FreedomFabric™ Graphical User Interface (GUI) for the first time, and provide the network-configuration parameters for the Acopia Adaptive Resource Switch (ARX).

Before you begin, perform the initial-boot process as described in the appropriate Hardware Installation manual: *ARX®500 Hardware Installation Guide*, *ARX®1000 Hardware Installation Guide*, or *ARX®6000 Hardware Installation Guide*. These manuals describe how to set up the out-of-band (OOB) management interface, along with a username and password for an administrative account.

Connecting to the GUI

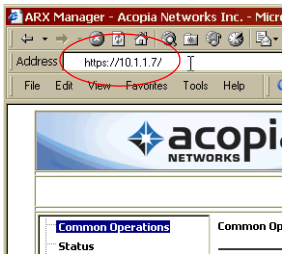
The ARX is initially provisioned to accept Secure HTTP (HTTPS) access over its OOB interface. Use the IP address for the OOB in an HTTPS URL:

https://*oob-address*/

where ***oob-address*** is the IP address configured during the initial-boot process.

You must access the ARX from a host on the OOB network, which *must* be separate from any subnet with clients and servers. The Initial Setup wizard (described below) creates another management interface that you can later access from the client/server network.

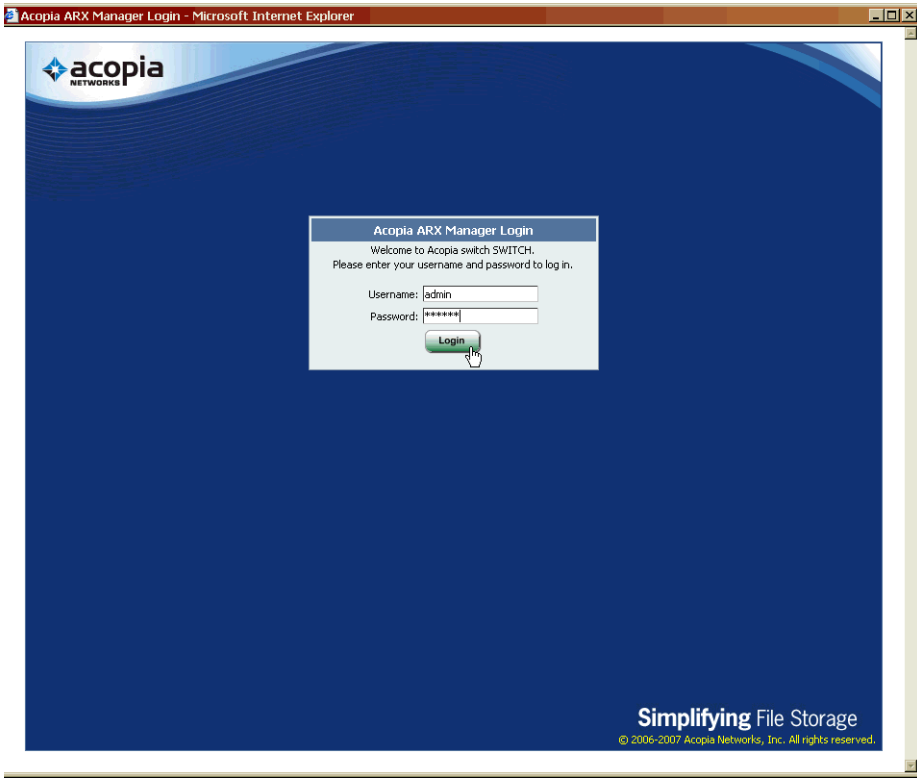
For example, this connects to the ARN manager at 10.1.1.7:



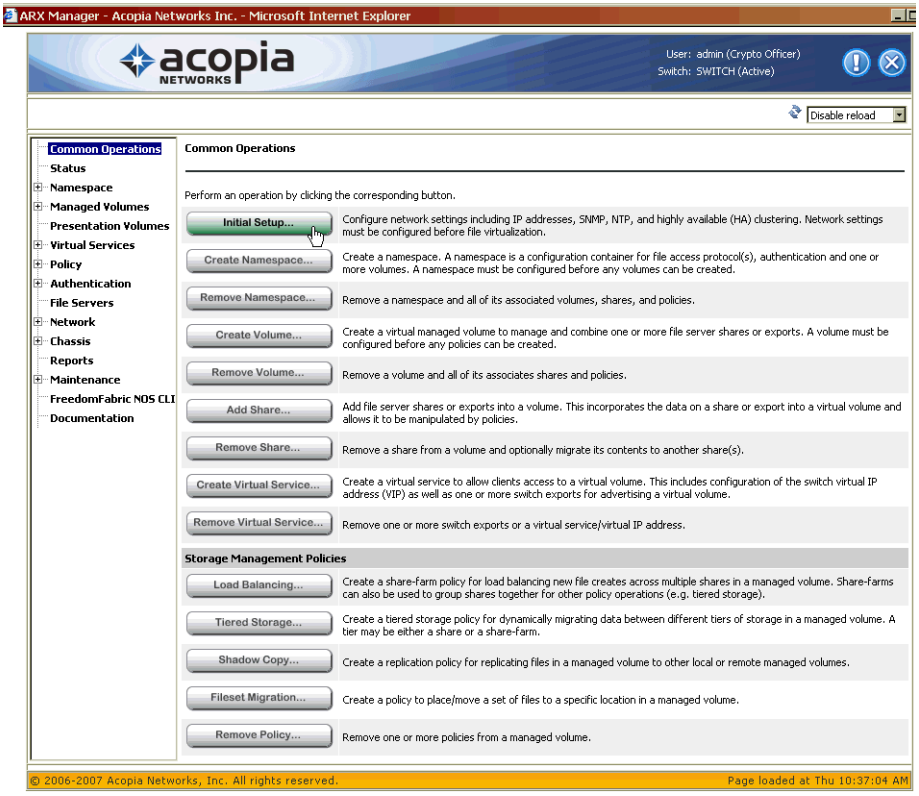
A security-alert pop-up appears the first time you access the GUI. This is to confirm that you trust the ARX as an HTTPS server. Click **yes** to proceed:

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

The GUI challenges you for a login name and a password. Use the name and password created during the initial-boot process. The default username for administration is "admin," though the installer has the option to choose any name.

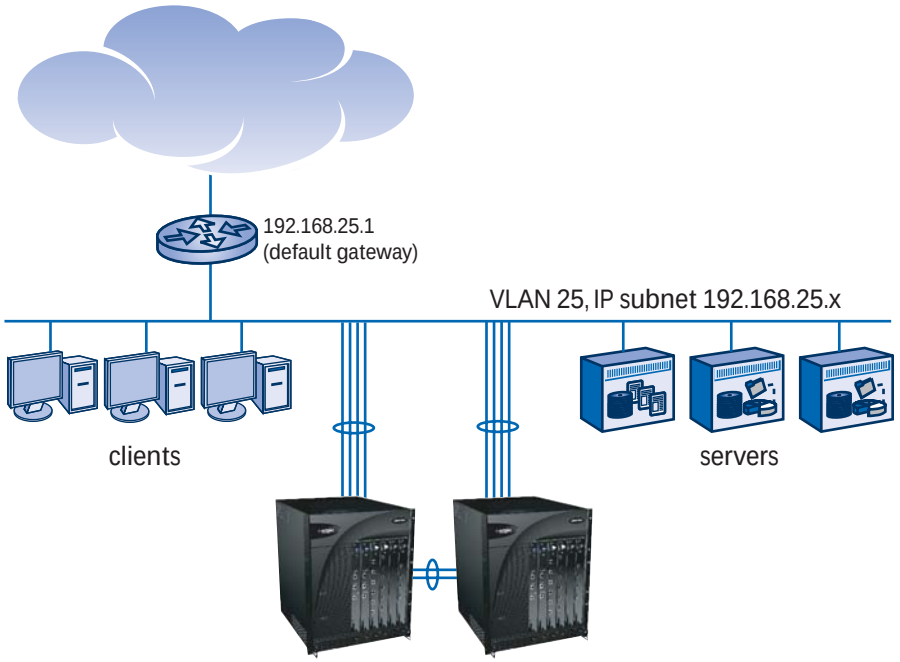

Acopia ARX Manager Login - Microsoft Internet Explorer
acopia
NETWORKS
Acopia ARX Manager Login
Welcome to Acopia switch SWITCH.
Please enter your username and password to log in.
Username: admin
Password: ******
Login
Simplifying File Storage
© 2006-2007 Acopia Networks, Inc. All rights reserved.

This invokes the GUI, at its Common Operations page. The GUI has a navigation panel on the left and a menu of wizards on the right. The button for the Initial Setup wizard is highlighted. Click on this button to begin initial configuration of the ARX:


ARX Manager - Acopia Networks Inc. - Microsoft Internet Explorer
acopia NETWORKS
User: admin (Crypto Officer)
Switch: SWITCH (Active)
Disable reload
Common Operations
Status
Namespace
Managed Volumes
Presentation Volumes
Virtual Services
Policy
Authentication
File Servers
Network
Chassis
Reports
Maintenance
FreedomFabric NOS CLI
Documentation
Common Operations
Perform an operation by clicking the corresponding button.
Initial Setup...
Configure network settings including IP addresses, SNMP, NTP, and highly available (HA) clustering. Network settings must be configured before file virtualization.
Create Namespace...
Create a namespace. A namespace is a configuration container for file access protocol(s), authentication and one or more volumes. A namespace must be configured before any volumes can be created.
Remove Namespace...
Remove a namespace and all of its associated volumes, shares, and policies.
Create Volume...
Create a virtual managed volume to manage and combine one or more file server shares or exports. A volume must be configured before any policies can be created.
Remove Volume...
Remove a volume and all of its associates shares and policies.
Add Share...
Add file server shares or exports into a volume. This incorporates the data on a share or export into a virtual volume and allows it to be manipulated by policies.
Remove Share...
Remove a share from a volume and optionally migrate its contents to another share(s).
Create Virtual Service...
Create a virtual service to allow clients access to a virtual volume. This includes configuration of the switch virtual IP address (VIP) as well as one or more switch exports for advertising a virtual volume.
Remove Virtual Service...
Remove one or more switch exports or a virtual service/virtual IP address.
Storage Management Policies
Load Balancing...
Create a share-farm policy for load balancing new file creates across multiple shares in a managed volume. Share-farms can also be used to group shares together for other policy operations (e.g. tiered storage).
Tiered Storage...
Create a tiered storage policy for dynamically migrating data between different tiers of storage in a managed volume. A tier may be either a share or a share-farm.
Shadow Copy...
Create a replication policy for replicating files in a managed volume to other local or remote managed volumes.
Fileset Migration...
Create a policy to place/move a set of files to a specific location in a managed volume.
Remove Policy...
Remove one or more policies from a managed volume.
© 2006-2007 Acopia Networks, Inc. All rights reserved.
Page loaded at Thu 10:37:04 AM

Setting Up Network Parameters

The Initial Setup wizard guides you through the process of setting up a one-armed-proxy network configuration. In a one-armed topology, the ARX connects to a single IP subnet and VLAN. All clients and file servers reside on this subnet or are reachable through a single default gateway. All client/server ports are typically aggregated into a channel. If you purchase a redundant ARX, some other ports are used in a *redundancy link* to connect the two ARXes.



The following screens guide you through the process of setting up a one-armed network configuration:

1. the hostname and high-level management access;
2. active client/server ports and their VLAN;
3. IP-address parameters, such as a new management-IP address on the above VLAN, proxy-IP addresses (used by the ARX to communicate with back-end file servers), and a default IP gateway;
4. a connection to the NTP server(s) used by file servers and client machines;
5. configuration for DNS lookups (optional);
6. an SMTP server and E-mail address(es) for E-mail alerts (optional);
7. SNMP trusted host, community string, and trap destination; and
8. redundancy configuration, if you previously purchased and installed a redundant ARX.

The final screen in the wizard summarizes all of the selections from the previous screens. If you confirm at this screen, the ARX commits all of the parameters. You cannot re-run this wizard unless you first re-run the initial-boot process; after you confirm, you can only make network-configuration changes from the CLI.

Information Checklist

Gather the following network information before you invoke the wizard:

- the IP subnet and VLAN for the ARX, containing
  - a new management IP for the ARX and
  - new proxy-IP addresses for the ARX (1 for an ARX®500, 4 for an ARX®1000, and 6 per ASM for an ARX®6000);
- the IP address(es) of the local NTP server(s);
- if you want optional E-mail alerts for alarms,
  - the IP address of the local DNS server and
  - the IP address of the local SMTP (E-mail) server;
- the IP address of the SNMP management station that will manage the ARX; and

- the IP address of a machine to receive the ARX's SNMP traps.

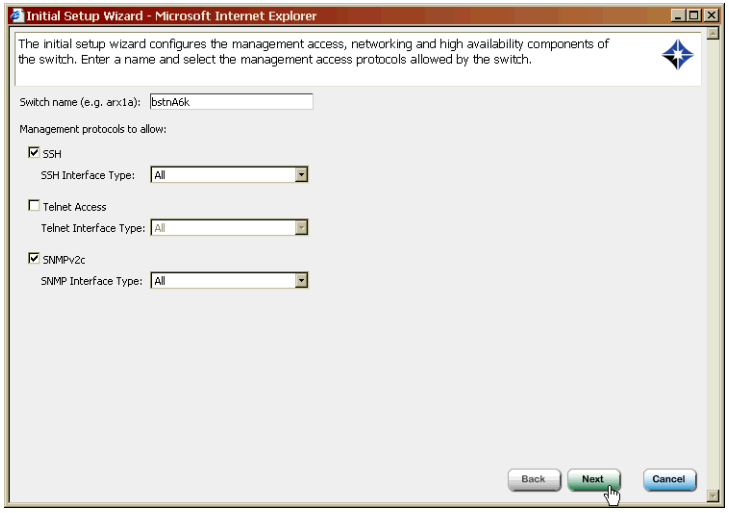
The following sections show each screen and a sample configuration.

Naming the ARX and Configuring Management Access

The first screen asks for a host name for the ARX.

You can also use the first screen to enable or disable management access through SSH, Telnet, and/or SNMPv2c. For each management protocol, you can choose a type of interface to allow: Management indicates the out-of-band (OOB) management interface and VLAN indicates any in-band (VLAN) management interface. VLAN access comes from the client/server network(s), and Management access comes from a disjoint management network. Choose either type of management interface, or all management interfaces.

Provide this information and click Next. For example, this is for a switch named "bstnA6k" which allows management access through SSH and SNMP:



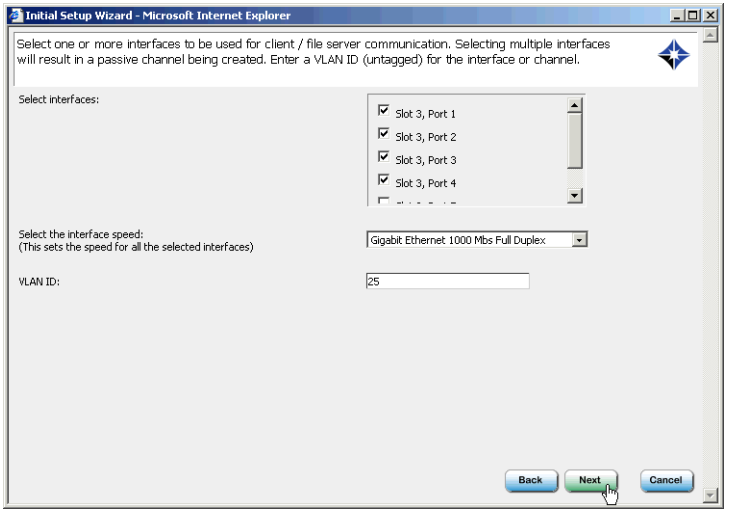
Configuring Physical Ports

The next screen sets up the physical-Ethernet ports, called “interfaces” in the GUI and CLI. Use this screen to enable one or more client/server ports, set their speed, and assign them to a VLAN. If you select more than one port, the GUI aggregates the ports into a channel.

NOTE

The ARX supports static (non-LACP) link aggregation only. The L2 switch at the other end of the channel must also support static aggregation. Further, it must include the same ports and belong to the same VLAN. Cable this channel and configure it at the other station before finishing this wizard.

For example, this ARX aggregates four ports into a channel over VLAN 25:


Initial Setup Wizard - Microsoft Internet Explorer
Select one or more interfaces to be used for client / file server communication. Selecting multiple interfaces will result in a passive channel being created. Enter a VLAN ID (untagged) for the interface or channel.
Select interfaces:
Slot 3, Port 1
Slot 3, Port 2
Slot 3, Port 3
Slot 3, Port 4
Select the interface speed:
(This sets the speed for all the selected interfaces)
Gigabit Ethernet 1000 Mbs Full Duplex
VLAN ID:
25
Back
Next
Cancel

Configuring IP Interfaces

The next screen configures the IP addresses for the ARX. All of these addresses must be on a common subnet over the VLAN you specified in the previous screen:

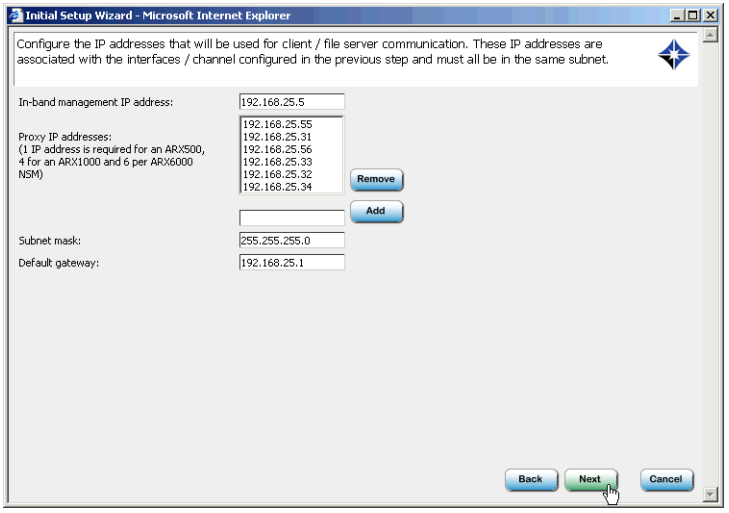
In-band management IP address is a management address that is accessible through the client/server VLAN configured above. Future connections to the GUI can come through this in-band management interface, from a client or server subnet instead of a separate management network.

Proxy IP addresses are used by the ARX to communicate with the file servers. The correct number of proxy-IP addresses varies from platform to platform; follow the on-screen instructions to add the correct number of addresses. These addresses must be on the client/server VLAN configured above, and all back-end file servers must be on the same subnet or reachable through the Default Gateway (below).

Subnet mask is the IP-subnet mask for all of the IP addresses on this screen.

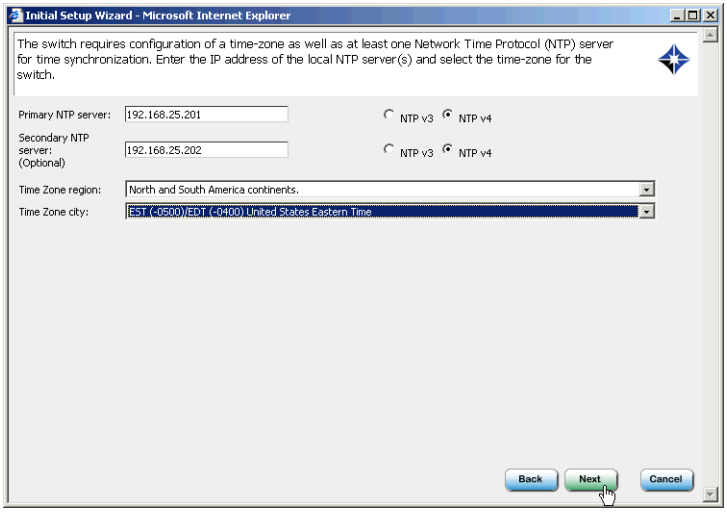
Default gateway identifies the local IP gateway that the ARX should use to reach all subnets outside the local proxy-IP subnet. Any clients or servers outside the proxy-IP subnet must be reachable through this gateway/router.

For example, this ARX has an in-band management address at 192.168.25.5, uses 6 proxy-IP addresses, and has a default gateway at 192.168.25.1:


Initial Setup Wizard - Microsoft Internet Explorer
Configure the IP addresses that will be used for client / file server communication. These IP addresses are associated with the interfaces / channel configured in the previous step and must all be in the same subnet.
In-band management IP address:
192.168.25.5
Proxy IP addresses:
(1 IP address is required for an ARX500, 4 for an ARX1000 and 6 per ARX6000 NSM)
192.168.25.55
192.168.25.31
192.168.25.56
192.168.25.33
192.168.25.32
192.168.25.34
Remove
Add
Subnet mask:
255.255.255.0
Default gateway:
192.168.25.1
Back
Next
Cancel

Connecting to the NTP Server

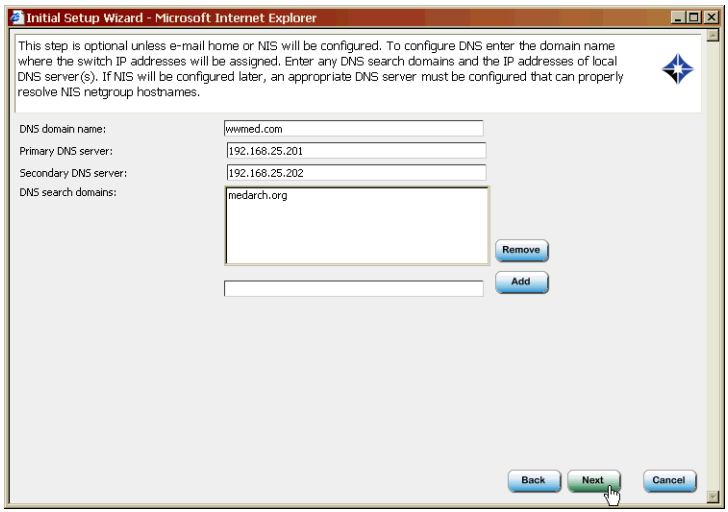
The next screen requires the IP address of your installation's Network Time Protocol (NTP) server. This must be the NTP server that is used by all servers and client machines on your network. Consistent time management is crucial for file-placement policy, Kerberos authentication, and many other ARX features. You also set the local time zone on this screen. For example, this switch uses an NTP server at 192.168.25.201 (along with a secondary server at 192.168.25.205) and uses the EST time zone:


Initial Setup Wizard - Microsoft Internet Explorer
The switch requires configuration of a time-zone as well as at least one Network Time Protocol (NTP) server for time synchronization. Enter the IP address of the local NTP server(s) and select the time-zone for the switch.
Primary NTP server:
192.168.25.201
NTP v3
NTP v4
Secondary NTP server: (Optional)
192.168.25.202
NTP v3
NTP v4
Time Zone region:
North and South America continents.
Time Zone city:
EST (-0500)/EDT (-0400) United States Eastern Time
Back
Next
Cancel

Setting Up DNS Lookups (optional)

The next screen identifies your local DNS server(s), so that the ARX can call them to translate IP addresses into host names. This is only necessary if you plan to configure E-mail alerts later. You can skip this screen if you do not plan to configure the system for E-mail alerts.

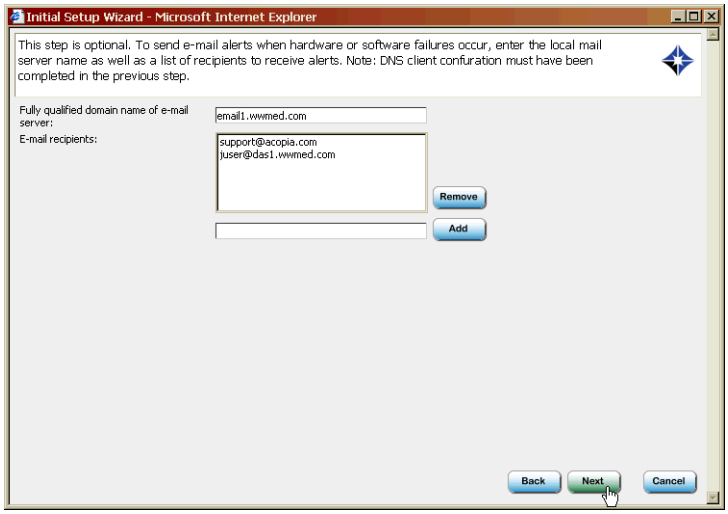
For example, this ARX has a primary DNS server and a secondary server, and uses two DNS-search domains:


Initial Setup Wizard - Microsoft Internet Explorer
This step is optional unless e-mail home or NIS will be configured. To configure DNS enter the domain name where the switch IP addresses will be assigned. Enter any DNS search domains and the IP addresses of local DNS server(s). If NIS will be configured later, an appropriate DNS server must be configured that can properly resolve NIS netgroup hostnames.
DNS domain name:
wwmed.com
Primary DNS server:
192.168.25.201
Secondary DNS server:
192.168.25.202
DNS search domains:
medarch.org
Remove
Add
Back
Next
Cancel

Configuring E-mail Alerts (optional)

As mentioned above, you can optionally configure the ARX to send alerts to E-mail recipients. Whenever a chassis-related alarm condition occurs that triggers an SNMP trap, these E-mail users receive a message. The *SNMP Reference* documents all possible SNMP traps and identifies the chassis-related traps. We strongly recommend that you configure the E-mail notification feature.

You use this next screen to identify the local E-mail server and one or more destination addresses. For example, this ARX uses an E-mail server at "email1.wwmed.com" and sends messages to two recipients:


Initial Setup Wizard - Microsoft Internet Explorer
This step is optional. To send e-mail alerts when hardware or software failures occur, enter the local mail server name as well as a list of recipients to receive alerts. Note: DNS client confuration must have been completed in the previous step.
Fully qualified domain name of e-mail server:
email1.wwmed.com
E-mail recipients:
support@acopia.com
juser@das1.wwmed.com
Remove
Add
Back
Next
Cancel

Setting Up SNMP Management

You can use the Simple Network Management Protocol (SNMP) for managing and monitoring ARX from one or more remote machines. Use the next screen to set up your SNMP parameters:

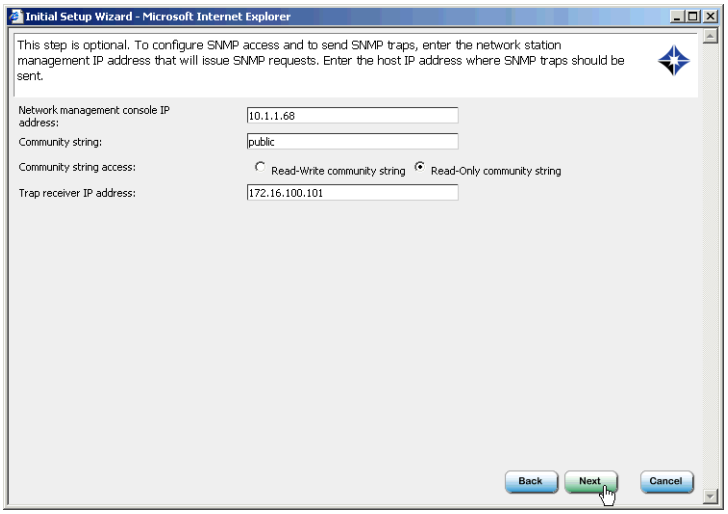
Network management console IP address identifies a host machine that you trust to perform SNMP "get" and "set' operations. This is typically a host that runs the network-management software for the site.

Community string is the community string to be used for SNMP "get" and "set" requests.

Community string access determines the privileges (read-only or read-write) for any “get” or “set” that uses the community string.

Trap receiver IP address is the host to receive all SNMP traps. For a complete list of SNMP traps from the ARX, see the *SNMP Reference*.

For example, this ARX allows “get” operations from a host at 10.1.1.68. The SNMP requests must use the “public” community string. Since that community string only allows read access, “set” operations are prohibited. Also, this ARX sends all of its SNMP traps to 172.16.100.101:


Initial Setup Wizard - Microsoft Internet Explorer
This step is optional. To configure SNMP access and to send SNMP traps, enter the network station management IP address that will issue SNMP requests. Enter the host IP address where SNMP traps should be sent.
Network management console IP address:
10.1.1.68
Community string:
public
Community string access:
Read-Write community string
Read-Only community string
Trap receiver IP address:
172.16.100.101
Back
Next
Cancel

Pairing with a Redundant ARX (optional)

You can use the final configuration screen to identify another ARX to be used as a redundant peer. This switch must have a matching hardware configuration, and must have been initially provisioned with redundancy in mind (as described in the Hardware Installation manuals). The screen contains the following fields:

Redundancy interface(s) are one or more interfaces used for the *redundancy link* between the peers. The peers use this link to exchange heartbeats and synchronization data. The link is typically a direct connection between the peers. If you select more than one port, the GUI creates a static (non-LACP) channel. The ARX®500 has a single, dedicated port for this purpose, 1/2.

Select the redundancy interface speed chooses a speed for the redundancy link. A Gigabit connection is required for optimal failover performance; 100Mbps connections are supported, but cause a longer interruption in service after a failover. If you directly connect the peers, use 1000Mbps (Gigabit) with full duplex.

Management IP address of peer switch is an in-band management address at the peer, or its OOB management address. This is used for the initial rendezvous between peer switches.

Quorum file server IP address identifies a file server to host the pair's quorum disk. The *quorum disk* is an external CIFS share or NFS export that provides an additional path for heartbeats; each peer writes its heartbeats to the quorum disk, and reads the other switch's heartbeat from the quorum disk. Choose a highly-available, high-performance file server, where the round-trip time for writing 1 block of data is less than 1 second. This file server must be reachable from the in-band management IP configured on an earlier screen.

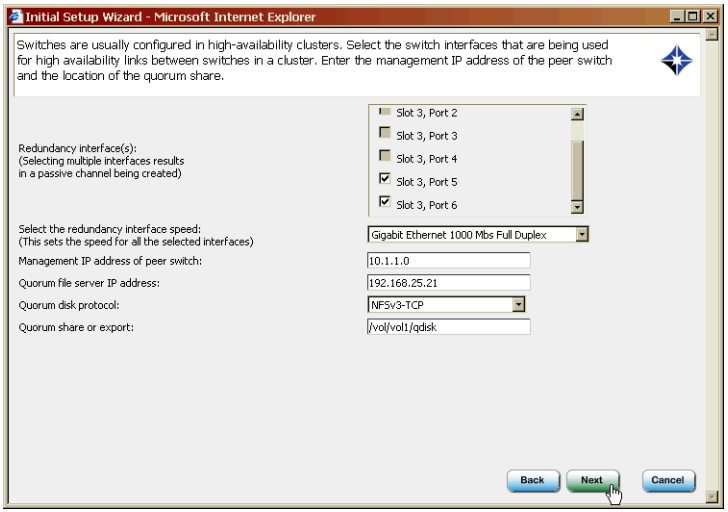
Quorum disk protocol is NFS or CIFS.

Quorum share or export identifies a dedicated share or export at the above file server. This share *cannot* be used for any storage services later, though other shares on the same file server may be used in storage services.

The remaining fields only apply to a CIFS share being used as the quorum disk; they disappear if you choose an NFS variant for the Quorum disk protocol above. A CIFS share requires proper authentication:

> CIFS quorum file-server username is a valid username. The ARX uses this identity to authenticate with the file server. Choose a username with permission to read from and write to the share.
>
> CIFS password is the above user's password.
>
> Confirm CIFS password asks for the password a second time, for confirmation.

For example, this ARX uses a 2-port channel to connect to a redundant switch at 10.1.1.8:

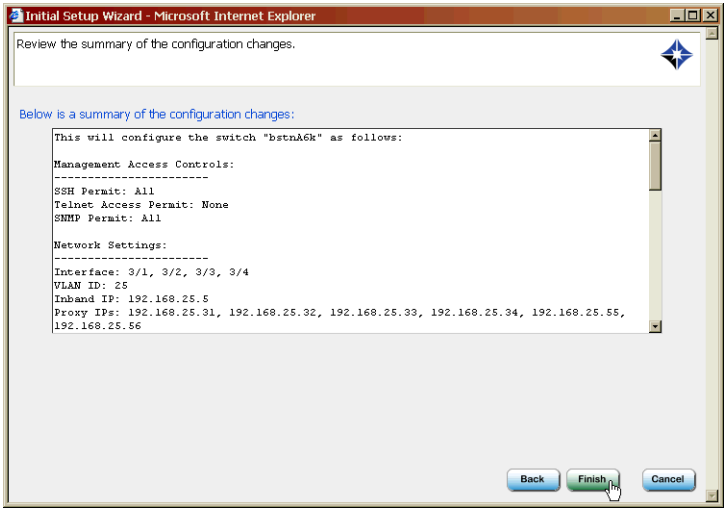

Initial Setup Wizard - Microsoft Internet Explorer
Switches are usually configured in high-availability clusters. Select the switch interfaces that are being used for high availability links between switches in a cluster. Enter the management IP address of the peer switch and the location of the quorum share.
Redundancy interface(s):
(Selecting multiple interfaces results in a passive channel being created)
Slot 3, Port 2
Slot 3, Port 3
Slot 3, Port 4
Slot 3, Port 5
Slot 3, Port 6
Select the redundancy interface speed:
(This sets the speed for all the selected interfaces)
Gigabit Ethernet 1000 Mbs Full Duplex
Management IP address of peer switch:
10.1.1.0
Quorum file server IP address:
192.168.25.21
Quorum disk protocol:
NFSv3-TCP
Quorum share or export:
/vol/vol1/qdisk
Back
Next
Cancel

NOTE

You must invoke this wizard on the peer switch, too. The peer switch must have the same visibility to all clients and servers so that it can support all of the same storage services. It should also share the same NTP server(s). However, it must have unique proxy-IP addresses, management-IP addresses, and hostname, so that you can manage it independently. The switches form a pair after you finish the Initial Setup wizard on both of them, as described in the next section.

Confirming

The last screen shows the total configuration from all of the previous screens. Review this information before continuing; after you confirm, you cannot re-run this wizard. To correct anything, click Back to return to any screen with misinformation, then click Next to go back to the confirmation screen. Click Finish when you are satisfied. For example:


Initial Setup Wizard - Microsoft Internet Explorer
Review the summary of the configuration changes.
Below is a summary of the configuration changes:
This will configure the switch "bstnA6k" as follows:
Management Access Controls:
SSH Permit: All
Telnet Access Permit: None
SNMP Permit: All
Network Settings:
Interface: 3/1, 3/2, 3/3, 3/4
VLAN ID: 25
Inband IP: 192.168.25.5
Proxy IPs: 192.168.25.31, 192.168.25.32, 192.168.25.33, 192.168.25.34, 192.168.25.55, 192.168.25.56
Back
Finish
Cancel

Further Network Configuration

The Initial Setup wizard provides all of the basic-networking configuration that is required for most installations. For additional client/server VLANs, static routes, multiple channels, or other complexity, you can use the CLI interface. To access and use the CLI to configure network settings, follow the instructions in the *CLI Network-Management Guide*. For a comprehensive listing of all CLI commands, refer to the *CLI Reference Guide*.

Setting Up Storage Services

The preceding section described the first wizard in the GUI's Common Operations page. You can use the remaining wizards to set up storage services on the ARX. These wizards are sufficient for most installations, and they introduce you to all of the major configuration objects in the GUI and CLI. To edit or expand the configurations later, you can use the detailed editing screens. These screens are accessible through the navigation panel on the left side of the screen.

The major storage-configuration components are namespaces, volumes, and virtual services. A *namespace* is a container for one or more volumes; it defines the protocol (NFS and/or CIFS) and authentication parameters that are common to its volumes. A *volume* aggregates the storage from one or more back-end file servers and is offered to clients as a single storage unit. A *virtual service* exposes a volume to NFS and/or CIFS clients. The *GUI Quick Start Guide: NFS Storage* explains how to set up NFS storage, and the *GUI Quick Start Guide: CIFS Storage* explains how to set up CIFS. To set up storage from the CLI, follow the instructions in the *CLI Storage-Management Guide*.

Once you have at least one volume configured and exposed through a virtual service, you can use storage-management policies to balance the storage load on your back-end file servers, arrange for tiers of storage, create a continuously-updated *shadow copy* of your volume, and/or migrate groups of files to file servers of your choosing. The wizards under Storage Management Policies lead you through the process of configuring each of these policies.

Contacting Customer Service

You can use the following methods to contact Acopia Customer Service:

E-mail	support@acopia.com
Telephone	1-866-4Acopia (1-866-422-6742)
Acopia TAC Online Acopia's online customer knowledge base and support request system	http://www.acopia.com/support/